

What Is Claimed Is:

1. A method of authenticating a user having a user privilege server proxy for a network system having a privilege server, a head end server and a web adapter comprising:
 - presenting user information to the web adapter from the user privilege server proxy;
 - presenting the user information to a head end server;
 - presenting the user information to the privilege server from the head end server;
 - validating the user in response to the user information;
 - when a user is validated, generating a ticket for the user at the privilege server;
 - providing the ticket to the user privilege server proxy through the head end server;
 - forming a service access request token from the ticket and user identification;
 - sending the token from the user to the privilege server;
 - validating the user in response to the token;
 - forming a packet having a sequence number, session key and the ticket at the privilege server;
 - providing the packet to the head-end server;
 - in response to the packet, authenticating the user at the head end server;
 - providing the packet to the user privilege proxy;

sending the ticket and sequence number encrypted with the session key to a service server through the web adapter;

5 validating the user at the service server; and

granting the user role based privileges at the service server.

2. A method as recited in claim 1 further comprising the step of negotiating the authentication
10 scheme between the server proxy and privilege server.

3. A method as recited in claim 1 wherein negotiating an authentication scheme between the server proxy and privilege server comprises presenting at least one security mechanism from the user privilege proxy
15 server to the privilege server; accepting or rejecting the at least one security mechanism at the privilege server.

4. A method as recited in claim 1 wherein the step of validating comprises validating in
20 accordance with the authentication scheme.

5. A method as recited in claim 1 further comprising the step of encrypting the ticket with a user password to form an encrypted ticket.

6. A method as recited in claim 1 further
25 comprising the step of decrypting the encrypted ticket at the user privilege server proxy.

7. A method as recited in claim 1 further comprising the steps of forming a packet having a sequence number and session key encrypted with the ticket at the privilege server decrypting the packet at the user privilege server proxy.

8. A method of authenticating a user having a user privilege server proxy for a network system having a privilege server, a head end server and a web adapter comprising:

10 negotiating an authentication scheme between the server proxy and privilege server;
presenting user information to the web adapter;
presenting the user information to a head end
15 server;
presenting the user information to the privilege server from the head end server;
validating the user at the privilege server in response to the user information in accordance with the
20 authentication scheme;
when a user is validated, generating a ticket for the user at the privilege server;
encrypting the ticket with a user password to form an encrypted ticket;
25 providing the encrypted ticket to the user privilege server proxy through the head end server;
decrypting the encrypted ticket;
forming a service access request token from the ticket and user identification at the user privilege
30 server proxy;
sending the token from the user privilege server proxy to the privilege server;

validating the user in response to the token;
forming a packet having a sequence number and
session key encrypted with the ticket at the privilege
server;
5 providing the packet to the head-end server;
in response to the packet, authenticating the
user at the head end server;
providing the packet to the user
privilege proxy;
10 decrypting the packet;
sending the ticket and sequence number
encrypted with the session key to a service server
through the web adapter;
validating the user at the service server; and
15 granting the user role based privileges at the
service server.

9. A method as recited in claim 8 wherein
negotiating an authentication scheme between the server
proxy and privilege server comprises presenting at least
20 one security mechanism from the user privilege proxy
server to the privilege server; accepting or rejecting
the at least one security mechanism at the privilege
server.

10. A method as recited in claim 8 wherein
25 the step of authenticating is performed by a policy
engine within the privilege server.

11. A method as recited in claim 8 wherein
generating a ticket comprises generating a ticket by
encrypting the user.

12. A method for accessing a service comprising:

presenting a ticket and sequence number to a service through the web adapter;

5 choosing a service in the service server;

sending the session name encrypted with the ticket and user identification to the privilege server and requesting a session key and sequence number;

receiving the session name from the user;

10 validating the user ticket and privilege;

when the user is validated, issuing the session key and sequence number for the ticket;

encrypting the session key and sequence number with the ticket to form a packet;

15 sending the packet and ticket to the service.

13. A system for authenticating a user having a user privilege server proxy for generating user information comprising:

20 a web adapter coupled to said user privilege server proxy for receiving user information;

a service server coupled to said web adapter;

an intermediate server coupled to the web adapter for receiving said user information;

25 a privilege server coupled to said intermediate server, said privilege server receiving said user information and validating said user in response to said user information, said privilege server generating a ticket;

30 said user privilege server proxy receiving said ticket through said intermediate server and generating a token;

said privilege server generating a packet having a sequence number and a session key in response to said token and coupling said packet to said user privilege server proxy;

5 said user privilege server proxy coupling the ticket and sequence number to said service server through said web adapter;

 said service server validating said user and granting said user privileges in response to the ticket
10 and session key.

14. A system as recited in claim 13 wherein said intermediate server comprises a head end server.

15 15. A system as recited in claim 13 wherein said user information comprises a user identification number.

16. A system as recited in claim 13 wherein said privilege server has a policy engine therein.

20 17. A system as recited in claim 16 wherein said privilege server comprises a key generator coupled to the policy engine.

18. A system as recited in claim 16 wherein said privilege server comprises a proxy coordinator coupled to the policy engine.

25 19. A system as recited in claim 16 wherein said privilege server comprises an obfuscator/deobfuscator coupled to the policy engine.

20. A system as recited in claim 16 wherein said privilege server comprises a store keeper coupled to the policy engine.

21. A system as recited in claim 20 wherein
5 said store keeper comprises a user information list and a session information list.

22. A system as recited in claim 13 wherein said service server validating said user and granting said user privileges in response to the ticket, session
10 key and sequence number.

23. A method of authenticating a user having a user privilege server proxy for a network system having a privilege server, a head end server and a web
15 adapter, said method comprising:

determining an authentication scheme at the privilege server;

validating the user at the privilege server in response to user information in accordance with the
20 authentication scheme;

when a user is validated, generating a ticket for the user at the privilege server;

encrypting the ticket with a user password to form an encrypted ticket;

25 validating the user in response to a service access request token formed from the ticket and a user identification; and

forming a packet having a sequence number and session key encrypted with the ticket at the privilege
30 server to authenticate the user.